Decrypted: HomuWitch Ransomware

Usage of the Decryptor

Please, read the following instructions carefully. The rate of success depends on them.

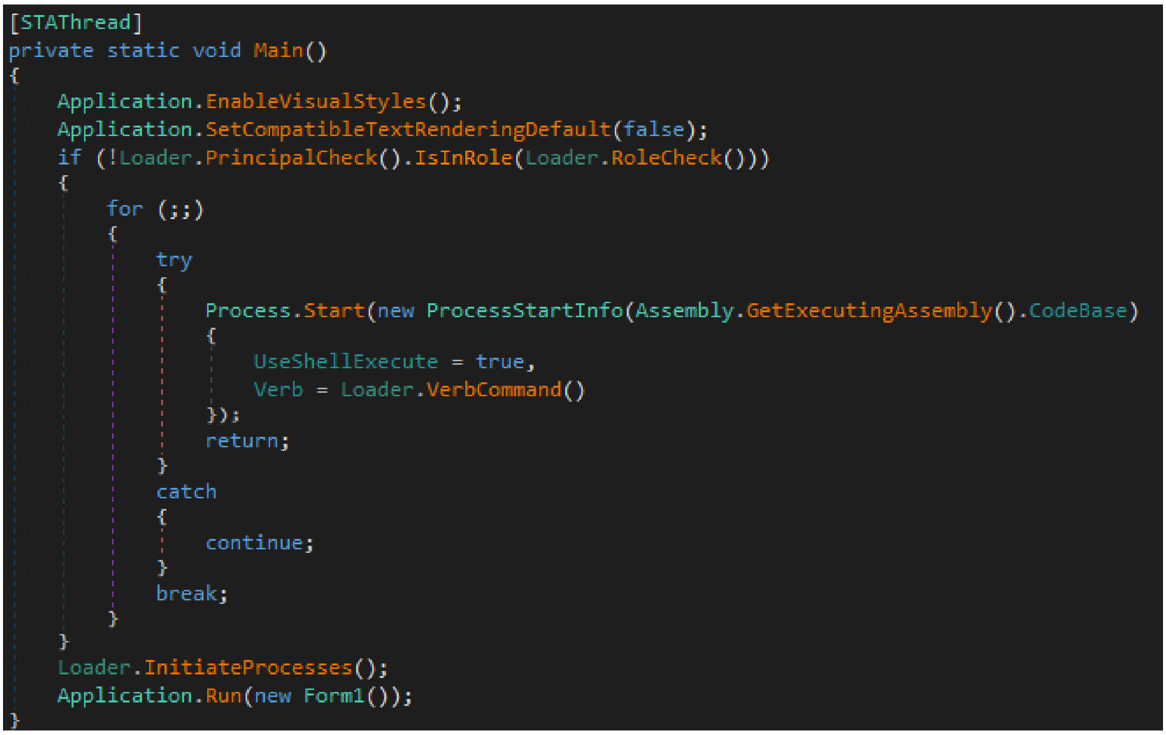
HomuWitch is a ransomware strain that initially emerged in July 2023. Unlike the majority of current ransomware strains, HomuWitch targets end-users – individuals – rather than institutions and companies. Its prevalence isn't remarkably large, nor is the requested ransom payment amount, which has allowed the strain to stay relatively under the radar thus far.

During our investigation of the threat, we found a vulnerability, which allowed us to create a free decryption tool for all the HomuWitch victims. We are now sharing this tool publicly to help impacted individuals decrypt their files, free of charge.

Despite a decrease in HomuWitch activity recently, we will continue to closely monitor this threat.

About HomuWitch

HomuWitch is a ransomware written in C# .NET. Its name comes from the file version information of the binary. Victims are usually infected via a SmokeLoader backdoor, masked as pirated software, which later installs a malicious dropper that executes the HomuWitch ransomware. Cases of infection are primarily found in two locations – Poland and Indonesia.



```
[STAThread]
private static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    if (!Loader.PrincipalCheck().IsInRole(Loader.RoleCheck()))
    {
        for (;;)
        {
            try
            {
                Process.Start(new ProcessStartInfo(Assembly.GetExecutingAssembly().CodeBase)
                {
                    UseShellExecute = true,
                    Verb = Loader.VerbCommand()
                });
                return;
            }
            catch
            {
                continue;
            }
            break;
        }
    }
    Loader.InitiateProcesses();
    Application.Run(new Form1());
}
```

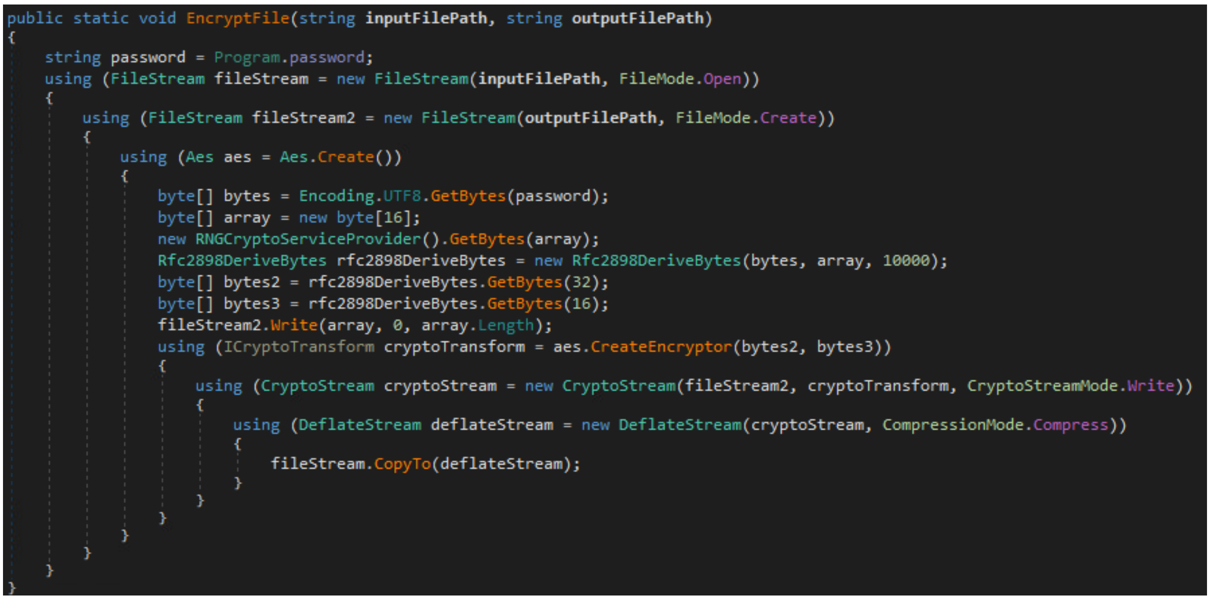
Overview of the dropper responsible for HomuWitch ransomware

HomuWitch Behavior

After the execution begins, drive letters are enumerated and those with a size smaller than 3,500 MB – as well as current user's directories for Pictures, Downloads, and Documents – are considered in the encryption process. Then, only files with specific extensions with size less than 55 MB are chosen to be encrypted. The list of the extensions contains following:

.pdf, .doc, .docx, .ppt, .pptx, .xls, .py, .rar, .zip, .7z, .txt, .mp4, .JPG, .PNG, .HEIC, .csv, .bbbbbbbbb

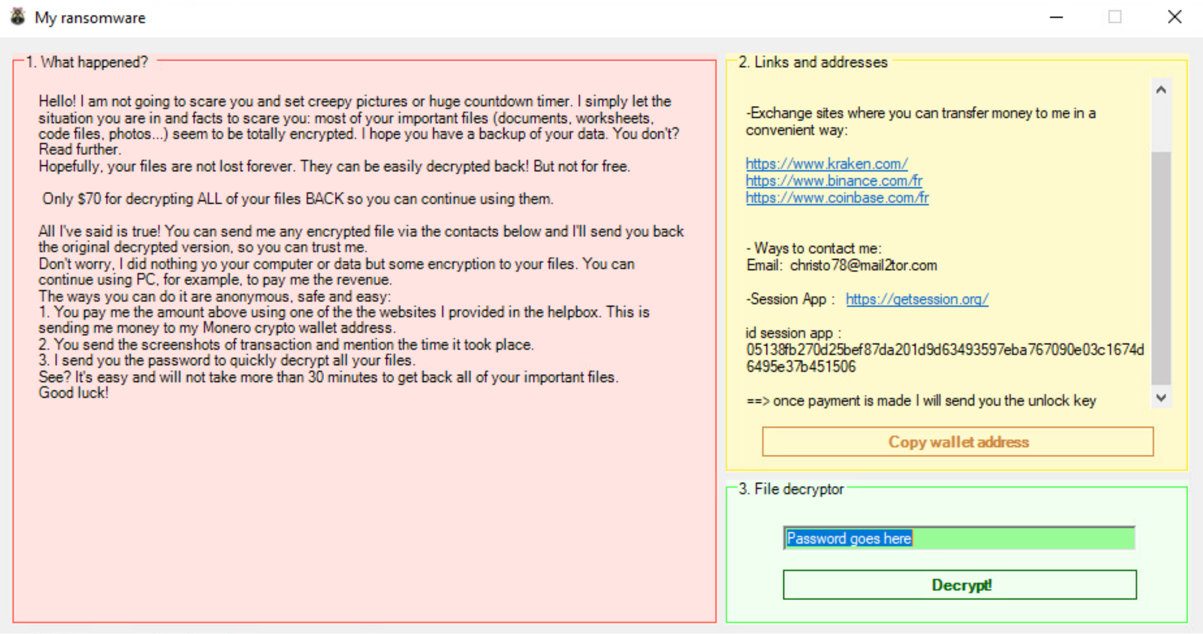
HomuWitch transforms the files with combination of Deflate algorithm for compression and AES-CBC algorithm for encryption, appending .homuencrypted extension to the filename. Most ransomware strains perform file encryption; HomuWitch also adds file compression. This causes the encrypted files to be smaller than originals.



```
public static void EncryptFile(string inputFilePath, string outputFilePath)
{
    string password = Program.password;
    using (FileStream fileStream = new FileStream(inputFilePath, FileMode.Open))
    {
        using (FileStream fileStream2 = new FileStream(outputFilePath, FileMode.Create))
        {
            using (Aes aes = Aes.Create())
            {
                byte[] bytes = Encoding.UTF8.GetBytes(password);
                byte[] array = new byte[16];
                new RNGCryptoServiceProvider().GetBytes(array);
                Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(bytes, array, 10000);
                byte[] bytes2 = rfc2898DeriveBytes.GetBytes(32);
                byte[] bytes3 = rfc2898DeriveBytes.GetBytes(16);
                fileStream2.Write(array, 0, array.Length);
                using (ICryptoTransform cryptoTransform = aes.CreateEncryptor(bytes2, bytes3))
                {
                    using (CryptoStream cryptoStream = new CryptoStream(fileStream2, cryptoTransform, CryptoStreamMode.Write))
                    {
                        using (DeflateStream deflateStream = new DeflateStream(cryptoStream, CompressionMode.Compress))
                        {
                            fileStream.CopyTo(deflateStream);
                        }
                    }
                }
            }
        }
    }
}
```

HomuWitch file-encryption routine

After encryption, a ransom note is either retrieved from the CnC server or (in some samples) is stored in the sample resources. The ransom typically varies $25 to $70, demanding the payment to be made with Monero cryptocurrency. Here is an example of HomuWitch ransom note:



Hello! I am not going to scare you and set creepy pictures or huge countdown timer. I simply let the situation you are in and facts to scare you: most of your important files (documents, worksheets, code files, photos...) seem to be totally encrypted. I hope you have a backup of your data. You don't? Read further.
Hopefully, your files are not lost forever. They can be easily decrypted back! But not for free.

Only $70 for decrypting ALL of your files BACK so you can continue using them.

All I've said is true! You can send me any encrypted file via the contacts below and I'll send you back the original decrypted version, so you can trust me.
Don't worry, I did nothing yo your computer or data but some encryption to your files. You can continue using PC, for example, to pay me the revenue.
The ways you can do it are anonymous, safe and easy:
1. You pay me the amount above using one of the the websites I provided in the helpbox. This is sending me money to my Monero crypto wallet address.
2. You send the screenshots of transaction and mention the time it took place.
3. I send you the password to quickly decrypt all your files.
See? It's easy and will not take more than 30 minutes to get back all of your important files.
Good luck!

-Exchange sites where you can transfer money to me in a convenient way:

https://www.kraken.com/
https://www.binance.com/fr
https://www.coinbase.com/fr

- Ways to contact me:
Email: christo78@mail2tor.com

-Session App : https://getsession.org/

id session app :
05138fb270d25bef87da201d9d63493597eba767090e03c1674d6495e37b451506

==> once payment is made I will send you the unlock key

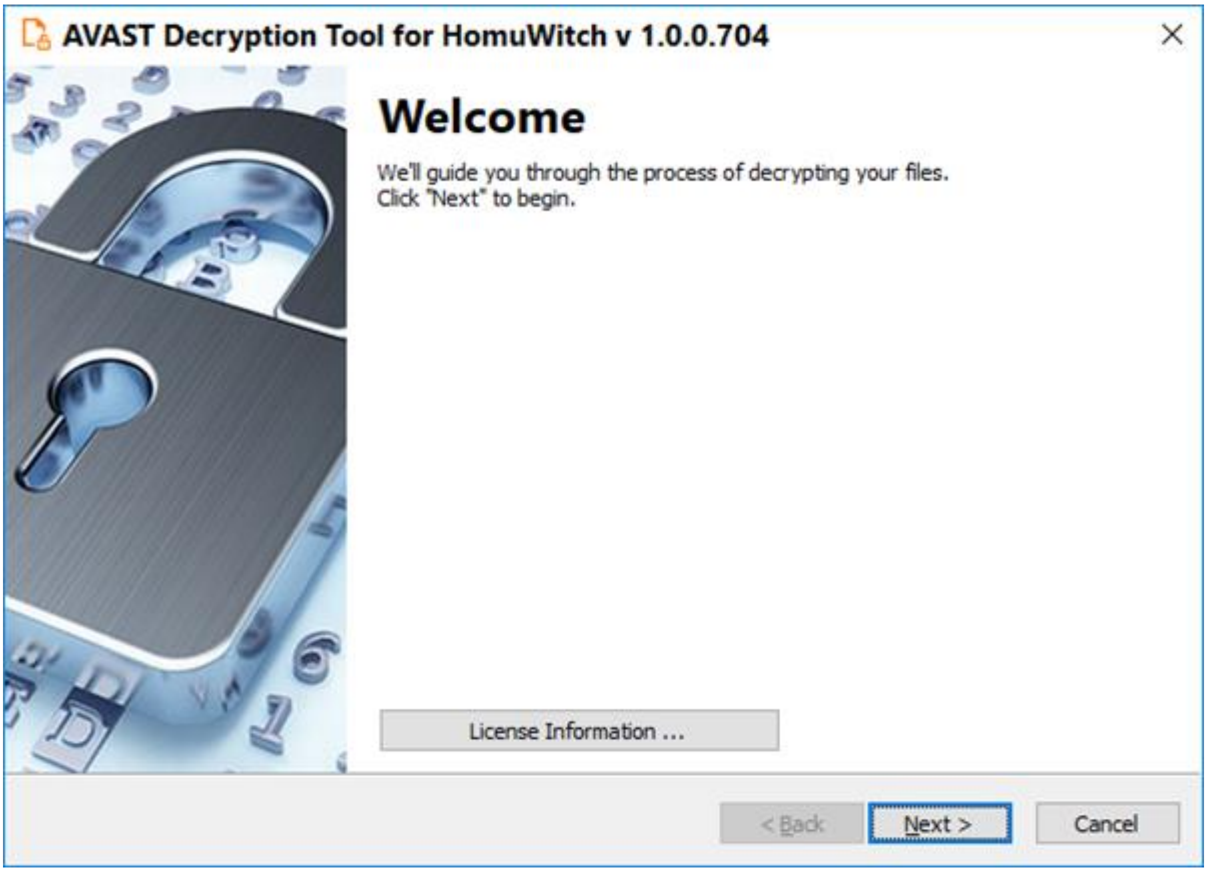
How to use the Avast HomuWitch ransomware decryption tool to decrypt files encrypted by the ransomware

Follow these steps to decrypt your files:

1. Download the free decryptor.

2. Run the executable file. It starts as a wizard, leading you through the configuration of the decryption process.

3. On the initial page, you can read the license information if you want, but you only need to click "Next".

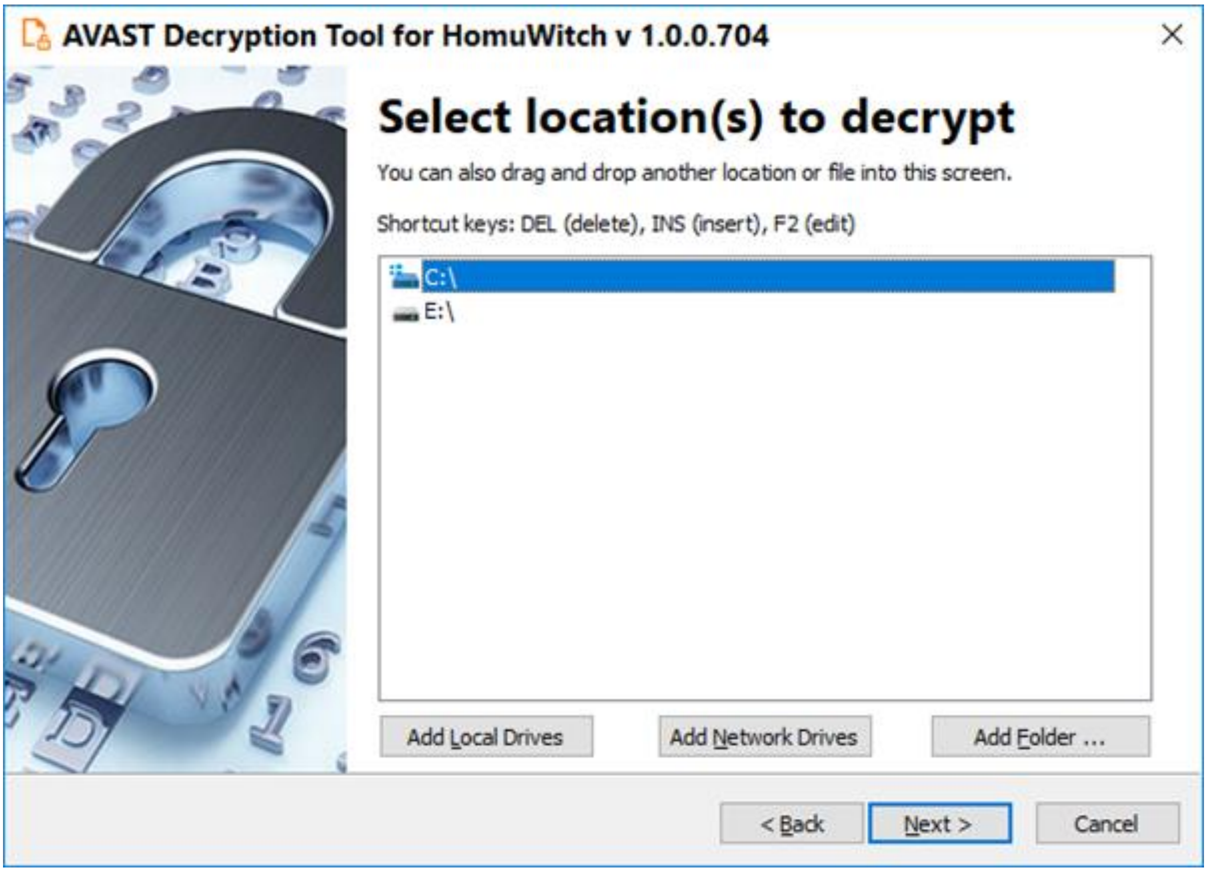


AVAST Decryption Tool for HomuWitch v 1.0.0.704

Welcome

We'll guide you through the process of decrypting your files.
Click "Next" to begin.

4. On the following page, select the list of locations you want to be searched for and decrypted. By default, it contains a list of all local drives:



AVAST Decryption Tool for HomuWitch v 1.0.0.704

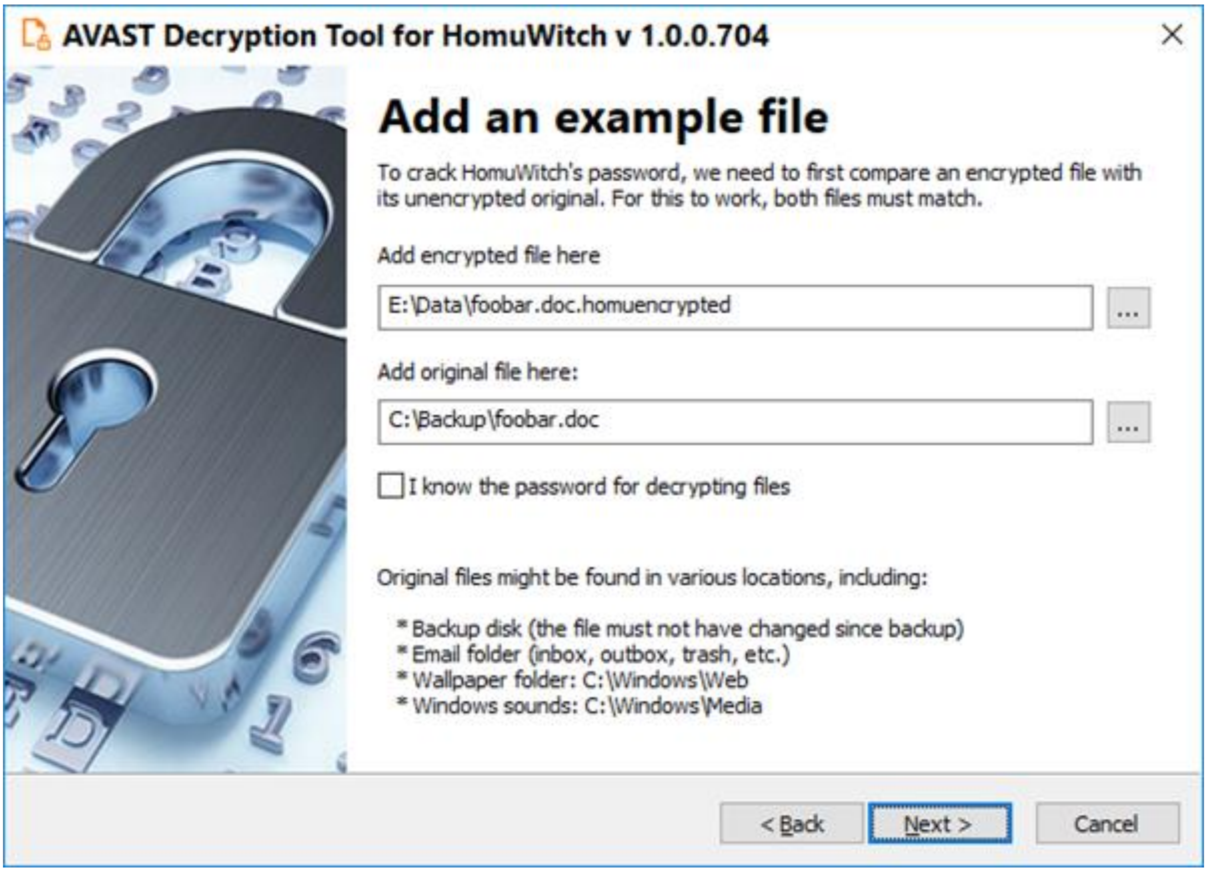
Select location(s) to decrypt

You can also drag and drop another location or file into this screen.

Shortcut keys: DEL (delete), INS (insert), F2 (edit)

C:\
E:\

5. On the third page, you need to provide a file in its original form and one which was encrypted by the HomuWitch ransomware. Enter both names of the files. If you have an encryption password created by a previous run of the decryptor, you can select "I know the password for decrypting files" option:



AVAST Decryption Tool for HomuWitch v 1.0.0.704

Add an example file

To crack HomuWitch's password, we need to first compare an encrypted file with its unencrypted original. For this to work, both files must match.

Add encrypted file here

E:\Data\foobar.doc.homuencrypted

Add original file here:

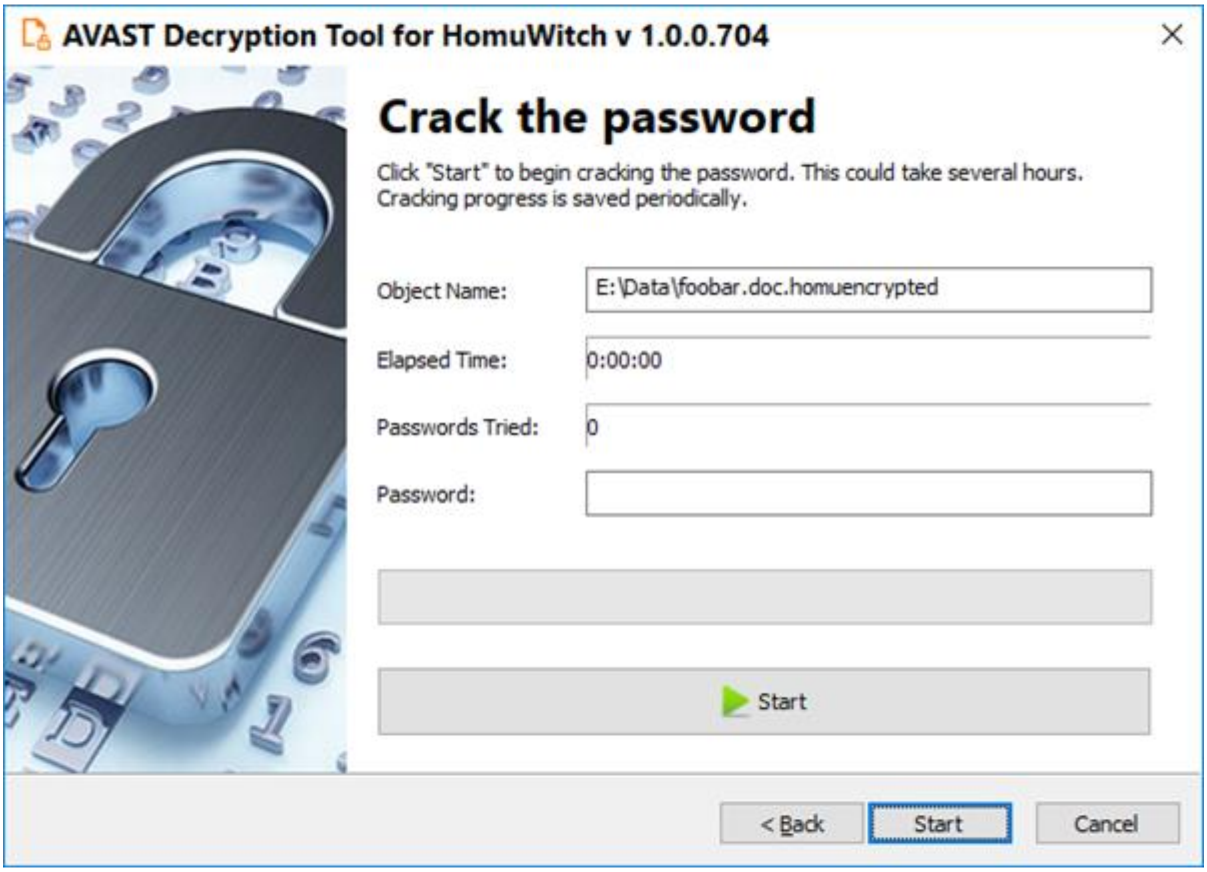
C:\Backup\foobar.doc

□ I know the password for decrypting files

Original files might be found in various locations, including:

* Backup disk (the file must not have changed since backup)
* Email folder (inbox, outbox, trash, etc.)
* Wallpaper folder: C:\Windows\Web
* Windows sounds: C:\Windows\Media

6. The next page is where the password cracking process takes place. Click “Start” when you are ready to start the process. The password cracking process uses all known HomuWitch passwords to determine the correct one.



AVAST Decryption Tool for HomuWitch v 1.0.0.704

Crack the password

Click "Start" to begin cracking the password. This could take several hours. Cracking progress is saved periodically.

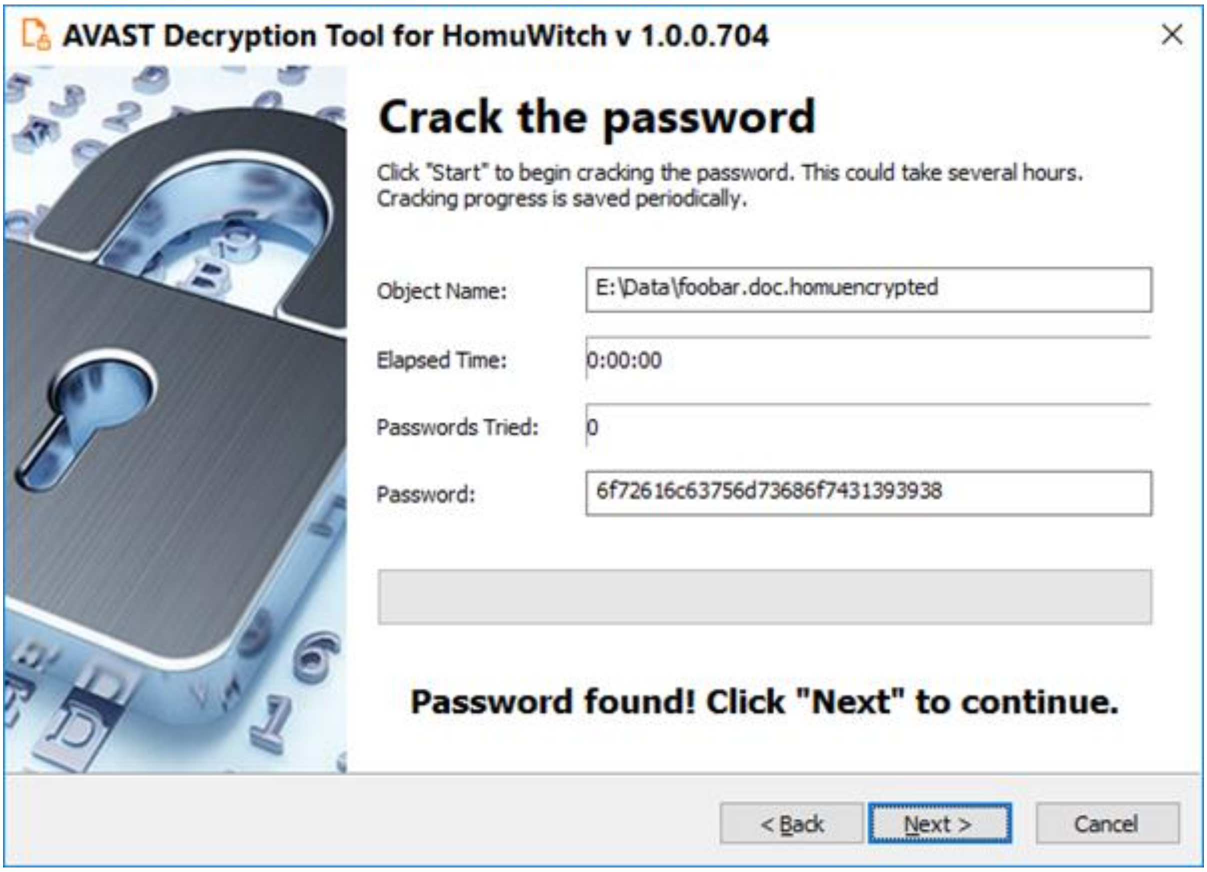
Object Name: E:\Data\foobar.doc.homuencrypted

Elapsed Time: 0:00:00

Passwords Tried: 0

Password:

7. Once the password is found, you can proceed to decrypt all the encrypted files on your PC by clicking “Next”.



AVAST Decryption Tool for HomuWitch v 1.0.0.704

Crack the password

Click "Start" to begin cracking the password. This could take several hours. Cracking progress is saved periodically.

Object Name: E:\Data\foobar.doc.homuencrypted

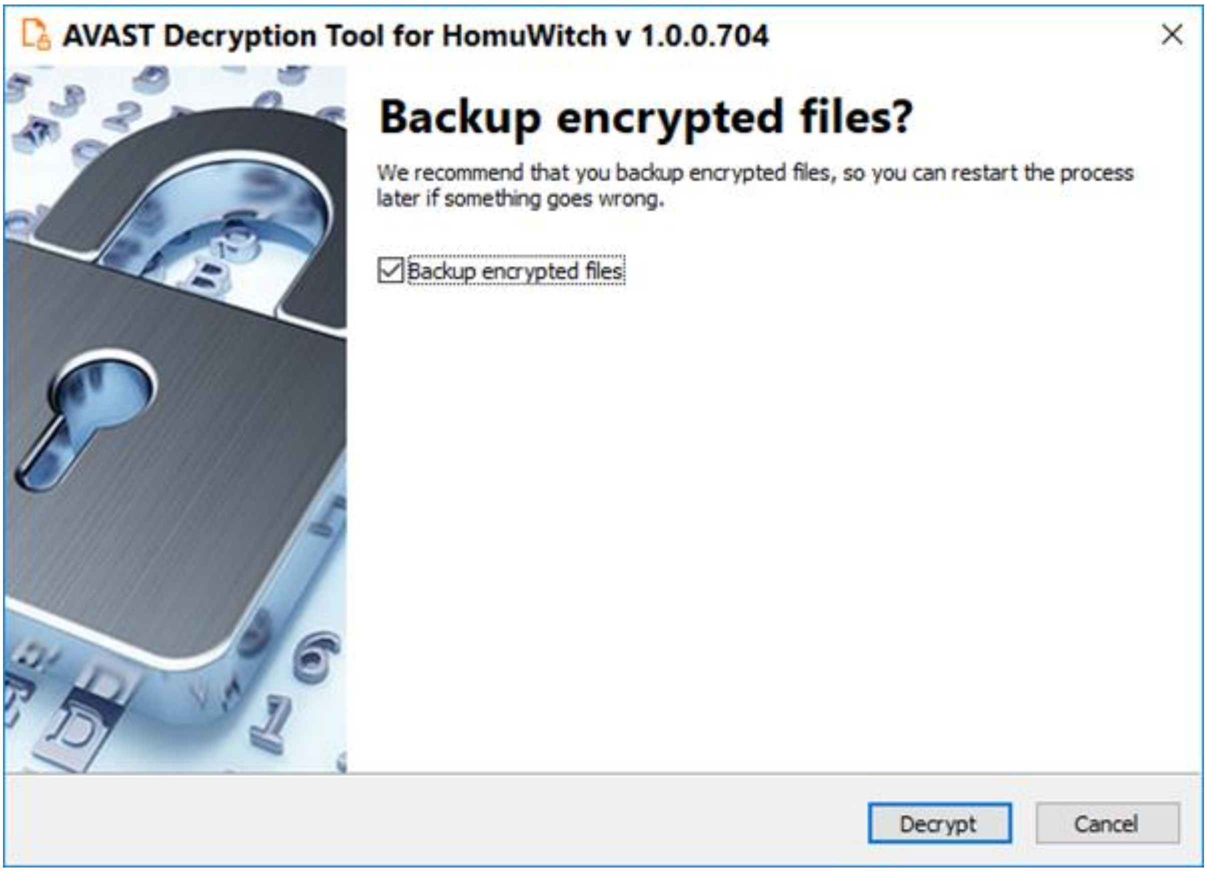
Elapsed Time: 0:00:00

Passwords Tried: 0

Password: 6f72616c63756d73686f7431393938

Password found! Click "Next" to continue.

8. On the final page, you can opt-in to back up your encrypted files. These backups may help if anything goes wrong during the decryption process. This option is on by default, which we recommend. After clicking "Decrypt" the decryption process begins. Let the decryptor work and wait until it finishes decrypting all of your files.



AVAST Decryption Tool for HomuWitch v 1.0.0.704

Backup encrypted files?

We recommend that you backup encrypted files, so you can restart the process later if something goes wrong.

☑ Backup encrypted files

Indicators of Compromise (IoCs)

Samples (SHA256)

03e4f770157c11d86d462cc4e9ebeddee3130565221700841a7239e68409accf

0e42c452b5795a974061712928d5005169126ad1201bd2b9490f377827528e5d

16c3eea8ed3a44ee22dad8e8aec0c8c6b43c23741498f11337779e6621d1fe4e

33dd6dfd51b79dad25357f07a8fb4da47cec010e0f8e6d164c546a18ad2a762c

3546b2dd517a99249ef5fd8dfd2a8fd80cb89dfdc9e38602e1f3115634789316

4ea00f1ffe2bbbf5476c0eb677ac75cf1a765fe5c8ce899f47eb8b344da878ed

6252cda4786396ebd7e9baf8ff0454d6af038aed48a7e4ec33cd9249816db2f4

9343a0714a0e159b1d49b591f0835398076af8c8e2da56cbb8c9b7a15c9707c8

bd90468f50629728d717c53cd7806ba59d6ad9377163d0d3328d6db4db6a3826

cd4c3db443dbfd768c59575ede3b1e26002277c109d39ea020d1bc307374e309

fd32a8c5cd211b057fdf3e7cc27167296c71e3fb42daa488649cdf81f58f6848

Command-and-Control Servers

IP Address	Origin
78.142.0.42	US
79.137.207.233	Germany
185.216.68.97	Netherlands
193.164.150.225	Russia

IoCs are available at https://github.com/avast/ioc/tree/master/HomuWitch